*Abdelhafid Boussouf University , Mila*
*Institute of Mathematics and computer science*
*Department of Computer Science*
*3rd Year Informatics*

***Year: 2025/2026***
***Computer Security***

# Directed Work N° 1

## Exercise 1:

Identify the security objectives that match these descriptions:

1. Which property guarantees that information remains accurate and unchanged unless altered by authorized individuals?
2. Which property prevents individuals from denying their actions and holds them accountable for what they've done?
3. Which property ensures that systems and information remain accessible to legitimate users whenever they need them?
4. Which property restricts information access to only those with proper permissions?
5. Which property verifies the identity of users before granting them access to systems or information?

## Exercise 2:

Identify the security service that will be affected in each of the following scenarios:

1. A hacker bombards a database server with endless queries.
2. An attacker successfully accessed a file in transit on the network. They can see its content but cannot decrypt it.
3. Air Algeria's database was attacked and all available seats on the London flight were reserved under the name "Security".
4. An attacker successfully accessed a file in transit on the network. They can see its content, decrypt and read it.
5. A user accidentally deletes a file and, to avoid sanctions, hides this action.
6. A hacker successfully uses an individual's credit card and purchases an iPhone on Apple's website.
7. Hackers inject content into a page that corrupts the target's browser. They can then modify the web page as they wish.
8. An attacker intercepts communication between two parties and relays messages between them, making them believe they are communicating directly.

## Exercise 3:

For each situation, identify and classify the threat based on the following criteria:

1. **Threat Source**: Internal or External
2. **Threat Agents**: Human, Environmental, or Technological
3. **Threat Motivation**: Malicious or Non-malicious
4. **Threat Intention**: Intentional or Accidental
5. **Threat Impacts**: Destruction, Corruption, Theft/Loss, Disclosure, Denial of Use, Elevation of Privilege, or Illegal Usage

**A.** A recently fired database administrator, still having system access during their notice period, deliberately deletes all customer records from the company's production database before leaving.

**B.** An employee receives an email appearing to be from the IT department asking them to verify their password by clicking a link. The employee clicks the link and enters their credentials, which are captured by cybercriminals who then access the company network.

**C.** Heavy rainfall causes flooding in the server room, damaging several servers and making critical business applications unavailable for three days.

**D.** Cybercriminals deploy ransomware across a hospital network, encrypting patient records and demanding $500,000 in cryptocurrency. The hospital cannot access patient histories, causing treatment delays.

**E.** A junior developer accidentally runs a DELETE query without a WHERE clause in the production database, removing 10,000 customer orders.

**F.** An employee working for a pharmaceutical company secretly photographs confidential drug formulas and sells them to a competitor for personal profit.

**G.** A bug in the accounting software causes it to incorrectly calculate tax amounts, resulting in wrong financial reports being sent to regulators.

**H.** A hacker exploits a vulnerability in the operating system to gain root/administrator access, allowing them to install backdoors and create new admin accounts.

**I.** An employee leaves their company laptop containing unencrypted customer data in a taxi. The laptop is never recovered.

## Exercise 4:

Match each scenario with its primary threat impact:

1. Hacker gains admin rights through exploit
2. Malware deletes all backup files
3. Employee emails customer list to competitor
4. Virus modifies financial records with random values
5. DDoS attack makes website unreachable
6. Employee uses company servers for personal cryptocurrency mining
7. Data breach exposes social security numbers